

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA

v.

(1) ERIC MEIGGS and
(2) DECLAN HARRINGTON,

Defendants

Criminal No. 19CR10438

Violations:

Count One: Conspiracy to Commit Computer Fraud and Abuse and Wire Fraud
(18 U.S.C. § 371)

Counts Two - Nine: Wire Fraud; Aiding and Abetting
(18 U.S.C. §§ 1343 and 2)

Count Ten: Computer Fraud and Abuse; Aiding and Abetting
(18 U.S.C. §§ 1030(a)((2), (c)(2)(B)(ii), and 2)

Count Eleven: Aggravated Identity Theft;
Aiding and Abetting
(18 U.S.C. §§ 1028A and 2)

Forfeiture Allegation:
(18 U.S.C. §§ 371, 981(a)(1)(C), 982(a)(2)(B),
1030(i) & 28 U.S.C. § 2461(c))

INDICTMENT

At all times relevant to this Indictment:

General Allegations

1. Defendant ERIC MEIGGS resided in the District of Massachusetts.
2. Defendant DECLAN HARRINGTON resided in the District of Massachusetts.
3. Victim 1 resided in New Jersey. Victim 1 published online guidance regarding cryptocurrency trading.
4. Victim 2 resided in Arizona. Victim 2 publicly communicated with cryptocurrency experts online.

5. Victim 3 resided in California. Victim 3 owned and operated a blockchain-based business.
6. Victim 4 resided in California and was a close friend of Victim 3's.
7. Victim 5 resided in California.
8. Victim 6 resided in Illinois. Victim 6 was leading a cryptocurrency project.
9. Victim 7 resided in Nevada. Victim 7 owned a Bitcoin Automated Teller Machine network.
10. Victim 8 resided in Michigan.
11. Victim 9 resided in California.
12. Victim 10 resided in California.

Definitions

13. A “SIM” card is an acronym for a Subscriber Identity Module card, which is a chip located inside a cell phone that stores information identifying and authenticating a cell phone subscriber. When a cell phone carrier reassigns a phone number from one physical phone to another—such as when a customer purchases a new phone but wants to retain the same number—the carrier switches the assignment of the cell phone number from the SIM card in the old phone to the SIM card in the new phone. This process is sometimes called “porting” a number. “SIM swapping” is a term for essentially the same process conducted without the authorization of the individual who legitimately controls the number. Cybercriminals generally engage in SIM swapping by convincing a victim’s cell phone carrier to reassign the victim’s cell phone number from the SIM card inside the victim’s cell phone to the SIM card inside a cell phone controlled by the cybercriminals. The process of convincing the cell phone carrier that

there is a legitimate reason for the switch is referred to as “social engineering.” For instance, the cybercriminal may pose as the victim and claim his cell phone was lost or damaged, and that he needs to have his number transferred to another phone. Alternatively, the cybercriminal may claim to be a representative of the carrier working at a local store, with a customer who needs to have their number ported to a new device. SIM swapping is not always accomplished through social engineering—some cybercriminals engage in SIM swapping by bribing or conspiring with an employee of the cell phone carrier, sometimes referred to as a “plug,” and having that employee make the switch.

14. An “account takeover” is a technique that cybercriminals use to take control of a victim’s online accounts (e.g., a victim’s email, social media, or cryptocurrency accounts) without authorization. Cybercriminals use a variety of techniques to conduct account takeovers. For example, cybercriminals who successfully SIM swap a victim may then pose as the victim with an online account provider and request that the provider send account password-reset links or an authentication code to the SIM-swapped device now controlled by the cybercriminals. The cybercriminals can then reset the victim’s account log-in credentials (e.g., username and password), even if the victim has tried to secure the account by requiring that an authentication code be sent (“two-factor authentication”). Cybercriminals can then use the log-in credentials to access the victim’s account without authorization, (i.e. “hack into” the account).

15. When users open accounts on social media platforms, such as Instagram or Twitter, they are generally asked to choose both a user name (also known as a “handle”) and a vanity name, which will also display on the account. Most social media platforms will allow multiple users to have the same vanity name, but the handle must be a unique identifier for each

user. For instance, there can be multiple Instagram users who have the display name “Shannon Sullivan,” but each account must have a different handle to identify the unique account (e.g., only one can be “@ShanS12345”). When a social media handle is an especially short, common, or well-known word or phrase, e.g. “@John,” or “@awesome,” the handle carries a particular cachet, because the ability to capture such a common word for individual use suggests that the user was an especially early adopter of that social media network. Such high value accounts are sometimes referred to as “OG accounts,” with “OG,” an acronym for “Original Gangster,” referring to veteran gang members, or in this case, veteran social media users. “OG accounts” are sometimes traded and/or offered for sale online.

16. Cryptocurrency is an umbrella term for a digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, generally with relative anonymity. Popular examples of cryptocurrencies include Bitcoin and Ethereum. Users maintain “wallets” and maintain online accounts with cryptocurrency exchanges such as Coinbase and Poloniex and Block.io. Because cryptocurrency wallets are often maintained online, users will generally create a phrase or list of words (called a “backup seed”) that can be used to recover their online wallets if necessary. The backup seed will allow the user to download the wallet software again and recover the cryptocurrency. However, possession of a backup seed by a cybercriminal would allow the criminal to take control of the online wallet.

17. Cybercriminals who engage in SIM swapping, account takeovers, and cryptocurrency theft often collaborate with one another online, using various online monikers, in underground forums like “OGUsers” and “Hackforums,” as well as using real-time

communications platforms.

Objects and Purpose of the Conspiracy

18. The objects of the conspiracy were: (1) to commit computer fraud by accessing and obtaining information from a protected computer in furtherance of a violation of criminal law; (2) to commit computer fraud by intentionally causing damage to a protected computer via the transmission of a program, information code or a command; and (3) to commit wire fraud. The purpose of the conspiracy was to obtain things of value from the victims, including, but not limited to, cryptocurrency and control of the victims' social medial accounts.

Manner and Means of the Conspiracy

19. Among the manner and means by which MEIGGS and HARRINGTON and co-conspirators known and unknown to the Grand Jury carried out the conspiracy were the following:

- a. Identifying potential victims who likely had significant amounts of cryptocurrency, for example, executives of cryptocurrency companies.
- b. Researching the potential victims using online tools.
- c. Engaging in "SIM swapping" in order to take control of victims' cell phone numbers.
- d. Leveraging their control over victims' cell phones to obtain unauthorized access to the victims' online accounts, including email accounts, social media accounts, and cryptocurrency accounts.
- e. Using their access to victims' accounts, to take control of, and steal things of value from the victims' online accounts, including their account handles and their cryptocurrency.

- f. Selling or otherwise transferring victims' log-in credentials, account handles, and cryptocurrency to others in exchange for money or other things of value.
- g. Using victims' hacked online accounts to communicate with the victims' friends and family in order to ask for money and cryptocurrency.
- h. Communicating with co-conspirators via online social media and chat platforms.
- i. Using multiple online accounts to hide their identities and evade detection by law enforcement.

Overt Acts in Furtherance of the Conspiracy and Acts in Furtherance of the Wire Fraud Scheme

Victim 1

20. On or about November 10, 2017, MEIGGS communicated online with others about targeting Victim 1 for SIM swapping and cryptocurrency theft. MEIGGS also shared email addresses belonging to Victim 1 and a SIM card number to which Victim 1's cell phone number could be SIM swapped.

21. On or about the same day, one or more members of the conspiracy SIM swapped Victim 1's cell phone number to a phone controlled by HARRINGTON.

22. On or about the same day, one or more members of the conspiracy caused password reset information and codes for Victim 1's accounts to be sent via text message to the phone controlled by HARRINGTON, including a text from Google.

23. On or about November 10, 2017, MEIGGS then accessed, without authorization, Victim 1's Gmail account and changed the password on the account. One or more members of the conspiracy then searched Victim 1's email for cryptocurrency wallet backup seeds, in an

attempt to access his cryptocurrency wallet and take possession of the funds.

24. On or about November 10, 2017, one or more members of the conspiracy also accessed, without authorization, Victim 1's Facebook account and, posing as Victim 1, used it to attempt to communicate with Victim 1's contacts.

25. On or about November 10, 2017, MEIGGS stated in his online communications that he had not successfully stolen any cryptocurrency from Victim 1.

Victim 2

26. On or about January 19, 2018, MEIGGS communicated online with others about targeting Victim 2 for SIM swapping and cryptocurrency theft.

27. On or about January 20, 2018, MEIGGS stated to others online that he would be willing to split the stolen cryptocurrency three ways. MEIGGS also provided Victim 2's email address to others online.

28. On or about the same day, one or more members of the conspiracy SIM swapped Victim 2's cell phone number to a phone controlled by HARRINGTON.

29. On or about the same day, one or more members of the conspiracy caused password reset information and codes to be sent via text message to the phone controlled by HARRINGTON.

30. On or about January 20, 2018, MEIGGS accessed, without authorization, Victim 2's Yahoo account, obtained information, and changed the account password. MEIGGS then provided the changed log-in credentials for Victim 2's Yahoo account to others online.

31. On or about January 20, 2018, MEIGGS also accessed or attempted to access, without authorization, Victim 2's Coinbase account, which contained approximately \$200,000 USD worth of cryptocurrency at the time. MEIGGS later told his co-conspirators that he was not

able to obtain funds from Victim 2.

Victims 3 and 4

32. On or about March 6, 2018, one or more members of the conspiracy SIM swapped Victim 3's cell phone number to a phone controlled by HARRINGTON.

33. On or about the same day, one or more members of the conspiracy caused password reset information and codes to be sent via text message to the phone controlled by HARRINGTON, including a text from Google.

34. On or about March 6, 2018, one or more members of the conspiracy accessed, without authorization, Victim 3's Gmail and Facebook accounts and changed the passwords for those accounts.

35. On or about March 6, 2018, one or more members of the conspiracy then posed as Victim 3 and used his Facebook account to send messages to Victim 3's contacts, fraudulently requesting funds. One or more members of the conspiracy convinced one of Victim 3's contacts, Victim 4, to send approximately \$100,000 USD worth of cryptocurrency to one or more members of the conspiracy.

Victim 5

36. On or about March 19, 2018, one or more members of the conspiracy SIM swapped Victim 5's cell phone number to a phone controlled by HARRINGTON.

37. On or about the same day, one or more members of the conspiracy caused password reset information and codes to be sent via text message to the phone controlled by HARRINGTON, including a text from Google.

38. One or more members of the conspiracy then accessed, without authorization,

Victim 5's Gmail account and his Yahoo account, which contained Victim 5's financial and personal identifying information, tax returns, and private passwords. They then changed the passwords on Victim 5's online accounts.

39. One or more members of the conspiracy further accessed, without authorization, Victim 5's LinkedIn, Facebook, and Twitter accounts, as well as his accounts at online cryptocurrency exchanges. One or more members of the conspiracy stole \$10,000 USD worth of cryptocurrency from Victim 5.

40. On or about March 20, 2018, one or more members of the conspiracy called Victim 5's wife from what appeared to be Victim 5's telephone number. They then sent a text message to Victim 5's daughter that read "TELL YOUR DAD TO GIVE US BITCOIN."

41. On or about March 20, 2018, one or more members of the conspiracy posed as Victim 5 and used at least one of Victim 5's social media accounts to send messages to Victim 5's contacts, fraudulently requesting cryptocurrency.

Victim 6

42. On or about May 4, 2018, one or more members of the conspiracy SIM swapped Victim 6's cell phone number to a phone controlled by HARRINGTON.

43. On the same day, one or more members of the conspiracy caused password reset information and codes to be sent via text message to the phone controlled by HARRINGTON, including a text from Google.

44. On the same day, one or more members of the conspiracy then accessed, without authorization, Victim 6's Gmail account and changed the password for the account.

45. One or more members of the conspiracy obtained from the Gmail account Victim

6's private key for a cryptocurrency wallet. They used the private key to steal over \$165,000 USD worth of cryptocurrency.

Victim 7

46. On or about May 8, 2018, one or more members of the conspiracy SIM swapped Victim 7's cell phone number to a phone controlled by HARRINGTON.

47. On or about the same day, one or more members of the conspiracy caused password reset information and codes to be sent via text message to the phone controlled by HARRINGTON, including a text from Google.

48. One or more members of the conspiracy then accessed, without authorization, Victim 7's personal and work email accounts, as well as his online Block.io cryptocurrency wallet.

49. On or about May 8, 2018, one or more members of the conspiracy stole approximately \$35,000 USD worth of cryptocurrency from Victim 7's Block.io cryptocurrency wallet.

Additional Wire Fraud By MEIGGS

Victim 8

50. In or about November and December of 2015, MEIGGS sent a series of online messages on Twitter and text messages to Victim 8, demanding that Victim 8 give MEIGGS control over Victim 8's Instagram handle, which was an OG account name. MEIGGS indicated he knew where Victim 8 lived by sending him his address, and then sent Victim 8 his mother's address and name, urging Victim 8 to "just give up."

51. On or about, November 30, 2015, MEIGGS called Victim 8 and threatened to kill Victim 8's wife if Victim 8 did not give up the Instagram handle. On or about December 2, 2015,

Victim 8 complied with MEIGGS' demands and changed the profile name on his account, which in turn allowed MEIGGS to control the victim's profile name.

Victim 9

52. On or about October 12, 2016, MEIGGS SIM swapped Victim 9's cell phone number. MEIGGS then called Victim 9 from Victim 9's own number and told him that he had convinced Victim 9's phone carrier to SIM swap his phone. MEIGGS told him that he wanted control of Victim 9's Tumblr account, which was an OG account. Victim 9 agreed to transfer control of the account in exchange for his phone number back.

53. On or about October 12, 2016, MEIGGS contacted Victim 9 by text messages and admitted that he had taken control of Victim 9's cell phone number.

Victim 10

54. On or about August 13, 2017, one or more individuals SIM swapped Victim 10's cell phone number.

55. On or about the same day, MEIGGS accessed, or attempted to access, without authorization, the Yahoo email account belonging to Victim 10, without Victim 10's authorization. One or more individuals then stole approximately \$20,000 worth of cryptocurrency from Victim 10's cryptocurrency wallet.

COUNT ONE

Conspiracy to Commit Computer Fraud and Abuse and Wire Fraud
(18 U.S.C. § 371)

The Grand Jury charges:

56. The Grand Jury re-alleges and incorporates by reference paragraphs 1-50 of this

Indictment.

57. From November 5, 2017 to November 13, 2019, in the District of Massachusetts, and elsewhere, the defendants,

(1) ERIC MEIGGS and
(2) DECLAN HARRINGTON,

conspired with each other and with others known and unknown to the Grand Jury to commit the following offenses:

- a. computer fraud and abuse, that is, intentionally accessing a protected computer without authorization and thereby obtaining information, in furtherance of any criminal and tortious act in violation of the laws of the United States, specifically wire fraud, in violation of Title 18, United States Code, Section 1343, all in violation of Title 18, United States Code, Sections 1030(a)(2) and (c)(2)(B)(ii);
- b. computer fraud and abuse, that is, knowingly causing the transmission of a program, information, code, and command, and as a result of such conduct, intentionally causing damage without authorization to a protected computer, in violation of Title 18 United States Code, Section 1030(a)(5)(A); and
- c. wire fraud, that is, having devised and intending to devise a scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations and promises, transmitting and causing to be transmitted, by

means of wire communications in interstate and foreign commerce, writings, signs, signals, pictures and sounds, for the purpose of executing the scheme to defraud, in violation of Title 18, United States Code, Section 1343.

All in violation of Title 18, United States Code, Section 371.

COUNTS TWO – FOUR
Wire Fraud
(18 U.S.C. § 1343)

The Grand Jury further charges:

58. The Grand Jury re-alleges and incorporates by reference paragraphs 1-18 and 51-56 of this Indictment.

59. On or about the dates set forth below, in the District of Massachusetts, and elsewhere, the defendant,

(1) ERIC MEIGGS,

having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of materially false and fraudulent pretenses, representations, and promises, did transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing the scheme to defraud, as set forth below:

Count	Approximate Date	Interstate Wire Communication
2	11/30/2015	Twitter communication from MEIGGS to Victim 8 regarding his Instagram Account
3	10/12/2016	Phone call from MEIGGS to Victim 9 regarding his Tumblr Account
4	8/13/2017	Access of Yahoo servers to change the password to Victim 10's Yahoo account

All in violation of Title 18, United State Code, Section 1343.

COUNTS FIVE – EIGHT
Wire Fraud
(18 U.S.C. § 1343)

The Grand Jury further charges:

60. The Grand Jury re-alleges and incorporates by reference paragraphs 1-50 of this Indictment.

61. On or about the dates set forth below, in the District of Massachusetts, and elsewhere, the defendant,

(2) DECLAN HARRINGTON,

having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of materially false and fraudulent pretenses, representations, and promises, did transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing the scheme to defraud, as set forth below:

Count	Approximate Date	Interstate Wire Communication
5	3/6/2018	Text from Google to Victim 3's phone number
6	3/19/18	Text from Google to Victim 5's phone number
7	5/4/2018	Text from Google to Victim 6's phone number
8	5/7/2018	Text from Google to Victim 7's phone number

All in violation of Title 18, United State Code, Section 1343.

COUNT NINE
Wire Fraud
(18 U.S.C. §§ 1343 and 2)

The Grand Jury further charges:

62. The Grand Jury re-alleges and incorporates by reference paragraphs 1-50 of this Indictment.

63. On or about the dates set forth below, in the District of Massachusetts, and elsewhere, the defendants,

(1) ERIC MEIGGS and
(2) DECLAN HARRINGTON,

aiding and abetting each other, having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of materially false and fraudulent pretenses, representations, and promises, did transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing the scheme to defraud, as set forth below:

Count	Approximate Date	Interstate Wire Communications
9	11/10/2017	Text from Google to Victim 1's phone number

All in violation of Title 18, United State Code, Section 1343 and Title 18, United States Code Section 2.

COUNT TEN
Computer Fraud and Abuse Act
(18 U.S.C. §§ 1030(a)(2) and (c)(2)(B)(ii) and 2)

The Grand Jury further charges:

64. The Grand Jury re-alleges and incorporates by reference paragraphs 1-50 of this Indictment.

65. On or about January 20, 2018, in the District of Massachusetts, and elsewhere, the defendants,

(1) ERIC MEIGGS and
(2) DECLAN HARRINGTON,

aiding and abetting each other, intentionally accessed a computer, namely the Oath service provider's computer associated with the Yahoo account of Victim 2, without authorization, and thereby obtained information from a protected computer, and the offense was committed in furtherance of any criminal and tortious act in violation of the laws of the United States, namely wire fraud in violation of Title 18, United States Code, Section 1343.

All in violation of Title 18, United State Code, Sections 1030(a)(2) and (c)(2)(B)(ii) and Title 18, United States Code, Section 2.

COUNT ELEVEN
Aggravated Identity Theft
(18 U.S.C. § 1028A and 2)

The Grand Jury further charges:

66. The Grand Jury re-alleges and incorporates by reference paragraphs 1-50 of this Indictment.

67. On or about January 20, 2018, in the District of Massachusetts, and elsewhere, the defendants,

- (1) ERIC MEIGGS and
- (2) DECLAN HARRINGTON,

during and in relation to a felony violation enumerated in subsection (c), specifically, 18 U.S.C. § 1030, as charged above in Count 10, knowingly transferred, possessed, and used, without lawful authority, a means of identification of another person, namely, the account log-in credentials of Victim 2.

All in violation of Title 18, United States Code, Sections 1028A and 2.

CONSPIRACY AND WIRE FRAUD FORFEITURE ALLEGATION
(18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c))

68. Upon conviction of one or more of the offenses in violation of Title 18, United States Code, Sections 371 and 1343, set forth in Counts One through Nine, the defendants,

(1) ERIC MEIGGS and
(2) DECLAN HARRINGTON,

shall forfeit to the United States, pursuant to Title 18, United States Code, Section 981(a)(1)(C), and Title 28, United States Code, Section 2461(c), any property, real or personal, which constitutes or is derived from proceeds traceable to the offenses.

69. If any of the property described in Paragraph 1, above, as being forfeitable pursuant to Title 18, United States Code, Section 981(a)(1)(C), and Title 28, United States Code, Section 2461(c), as a result of any act or omission of the defendants --

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the Court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be divided without difficulty;

it is the intention of the United States, pursuant to Title 28, United States Code, Section 2461(c), incorporating Title 21, United States Code, Section 853(p), to seek forfeiture of any other property of the defendants up to the value of the property described in Paragraph 1 above.

All pursuant to Title 18, United States Code, Section 981(a)(1)(C), and Title 28, United States Code, Section 2461(c).

COMPUTER FRAUD AND ABUSE ACT FORFEITURE ALLEGATION
(18 U.S.C. §§ 982(a)(2)(B) & 1030(i))

70. Upon conviction of the offense in violation of Title 18, United States Code, Section 1030(a)(2), set forth in Count Ten, the defendants,

- (1) ERIC MEIGGS and
- (2) DECLAN HARRINGTON,

shall forfeit to the United States, pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i), any property constituting, or derived from, any proceeds obtained, directly or indirectly, as a result of such offense; and any personal property used, or intended to be used, in any manner or part, to commit, or to facilitate the commission of, such offense.

71. If any of the property described in Paragraph 3, above, as being forfeitable to the United States, as a result of any act or omission of the defendants --

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the Court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be divided without difficulty;

it is the intention of the United States, pursuant to Title 18 United States Code, Sections 982(b)(2) and 1030(i)(2), each incorporating Title 21, United States Code, Section 853(p), to seek forfeiture of any other property of the defendant up to the value of the property described in Paragraph 3 above.

All pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i).

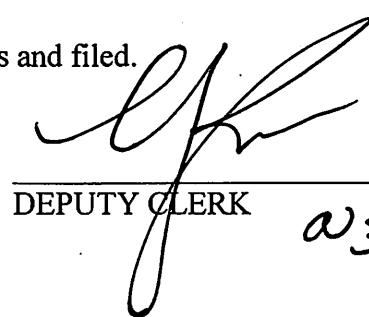
A TRUE BILL

FOREPERSON


AMY HARMAN BURKART
ASSISTANT UNITED STATES ATTORNEY
DISTRICT OF MASSACHUSETTS
MONA SEDKY
SENIOR TRIAL ATTORNEY
DEPARTMENT OF JUSTICE

District of Massachusetts: November 13, 2019

Returned into the District Court by the Grand Jurors and filed.



DEPUTY CLERK

23:40PM

SEALED